一种改进的基于奇偶校验码的 McEliece 变型方案 *

李梦东 [1,2]，孙玉情 [2]，韦依儿 [2]，程思培 [1]

(1. 北京电子科技学院，北京 100070; 2. 西安电子科技大学 通信工程学院，西安 710071)

摘　要：McEliece 公钥加密体制是基于编码理论的公钥密码体制，其安全性可以规约到一般线性码译码问题，可以抵抗量子攻击。提出了一种改进的基于准循环中密度奇偶校验（QC-MDPC）码和准循环低密度奇偶校验（QC-LDPC）码的 McEliece 变型方案。主要改进是将 QC-LDPC 码和 QC-MDPC 码的奇偶校验矩阵结合作为私钥，生成二者的级联码字应用于 McEliece 变型方案，并且给出了改进的译码算法。分析表明在 80 bit 安全下该体制密钥量小且实现的复杂度低，能抵抗最近提出的分别针对 QC-MDPC 和 QC-LDPC 体制的密钥恢复攻击。

关键词：准循环低密度奇偶校验码；准循环中密度奇偶校验码；McEliece 公钥体制；比特翻转译码算法

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2018.04.0349

Improved McEliece variant scheme based on parity-check codes

Li Mengdong[1, 2], Sun Yuqing[2], Wei Yier[2], Cheng Sipei[1]

(1. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 2. *Institute of Communication Engineering*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: McEliece public-key cryptosystem is a public-key cryptosystem based on coding theory. Its security can be reduced to the general linear code decoding problem and it can resist quantum attack. This paper proposed an improved McEliece variant scheme based on quasi-cyclic medium density parity check (QC-MDPC) code and quasi-cyclic low density parity check (QC-LDPC) code. The main improvement was that the parity check matrices of QC-LDPC code and QC- MDPC code were combined as a private key, and the concatenated codewords generated were applied to the McEliece variant scheme, and an improved decoding algorithm was given. The analysis shows that under the 80-bit security, it has small system key and low-implement complexity. In addition, this system can resist the recently proposed key recovery attacks on QC-MDPC and QC-LDPC respectively.

Key words: QC-LDPC; QC-MDPC; McEliece PKC; bit-flipping decoding algorithm

0　引言

近年来量子计算机发展迅速，为了避免量子攻击，选取后量子安全加密方案至关重要。基于纠错码的公钥密码体制，其安全性可以规约到一般线性码译码问题，是目前为止能够抵抗量子计算机攻击的主要方案之一，具有较好的安全性。经典的基于二元 Goppa 码编码的方案，例如 McEliece 和 Niderreiter 方案虽然实现速度很快，但存在密钥量大的问题。很多试图改进这一缺点的算法使用一些码代替 Goppa 码以得到更紧致的密钥表示，但大多已被攻破[1, 2]。目前较有希望的既保持安全性又具有较短密钥长度的 McEliece 变型算法是采用 QC-MDPC 码的方案。

Baldi 等人[3]最早将 QC-LDPC 码应用在 McEliece 体制中。这一没有过多代数结构同时具有快速译码算法的码，使加密体制既具有更小的公钥，又具有相应的安全性。但是不久这一算法被 Otmani 等人[4]利用结构攻击的方法攻破，原因是其对偶码存在低维数的漏洞。之后 Baldi 等人[5]又对其之前的 QC-LDPC 方案进行了改进，提高了安全性使其能抵抗 Otmani 的攻击。2013 年 Misoczki 等人[6]提出了采用 QC-MDPC 码的 McEliece 公钥密码体制，并证明其能够抵抗已知的对 LDPC 码的攻击，同时保持了 QC-LDPC 码密钥短的优点。但是在 2016 年，Guo 等人[7]对 Misoczki 提出的 QC-MDPC 方案提出了一种密钥恢复攻击，该攻击利用大量实验寻找译码错误概率和密钥距离谱之间的关联性，对密钥进行恢复。同年 Shooshtari 等人[8]证实了当

收稿日期：2018-04-23；**修回日期：**2018-07-12　　**基金项目：**北京市支持中央高校共建项目——青年英才计划项目；中央高校基本科研业务费专项资金资助项目（2017CL06）

作者简介：李梦东（1964-），男，山东利津人，教授，主要研究方向为密码算法及其应用；孙玉情（1990-），女，河南周口人，硕士研究生，主要研究方向为信息安全、密码学（18811300976@163.com）；韦依儿（1994-），女，陕西西安人，硕士研究生，主要研究方向为信息安全、密码学；程思培（1995-），男，山西长治人，硕士研究生，主要研究方向为保密通信．

Baldi 改进的 QC-LDPC McEliece 体制的循环矩阵的循环块为偶数时，其易遭受信息集译码攻击[8]。之后在 2017 年，Fabšič 等人[9]将 Guo 等人的攻击方法应用于该体制，同样是通过大量实验寻找置换矩阵 Q 与译码错误概率之间的依赖，对密钥进行恢复。

为了使 McEliece 变型体制能保持密钥短及传输率高的优点，并使其还能抵抗针对 QC-LDPC 与 QC-MDPC 变型体制的攻击，本文设计了将两种奇偶校验码结合使用的 McEliece 体制。利用密度不同的奇偶校验矩阵的合矩阵对生成矩阵进行定义，再对明文加密。密文为 QC-LDPC 和 QC-MDPC 码字的级联再加上随机差错图样 e，即 $c = mG + e$ 分析结果表明，在选择适当参数下，此体制可抵制 Guo 等人提出的密钥恢复攻击，同时也能避免针对 QC-LDPC 的攻击。

1　预备知识

1.1　相关定义

定义 1　LDPC 码。码字 $C = \{c \in F_2^n \mid Hc^T = 0\}$，是低密度奇偶校验码，其奇偶校验矩阵 H 密度较低，是个稀疏矩阵，可以用 Tanner 图来表示(见图 1)。

定义 2 MDPC 码。它是比 LDPC 码密度稍高的码，一个 (n,r,w) -MDPC 码是一个长度为 n，余维数为 $r(r<n)$ 的线性码，其奇偶校验矩阵具有恒定的行重 w。MDPC 码的奇偶校验矩阵的行列密度相比于 LDPC 码的奇偶校验矩阵稍高；实际中应用的 LDPC 码的奇偶校验矩阵行重一般情况下是小于等于 10 的，而 MDPC 码的奇偶校验矩阵的行重约为 $O(\sqrt{n\log n})$。一般对于 80 比特到 256 比特安全参数下，MDPC 码的校验矩阵选择的行重在 90 到 644 之间。

定义 3　准循环（quasi-cyclic，QC-）码。对于一个 (n,r) -线性码，若存在小整数 n_0（比如 2、3、4 等小整数），使得在这个码字集合中的每个码字每经过 n_0 的循环移位又生成一个码字，则称该码为准循环码。

定义 4　QC-LDPC/QC-MDPC 码。当 (n,r,w) -LDPC/MDPC 码字也是准循环时；或者说由循环块校验矩阵定义 (n,r,w) -LDPC/MDPC 码时，其中 $n = n_0 r$，则为准循环低/中密度奇偶校验码，即 QC-LDPC/QC-MDPC 码。

定义 5　循环矩阵。如果一个矩阵的行是第一行的连续循环移位，则称这个矩阵为循环矩阵。

定义 6　矩阵的密度 d_H。$H \in F_2^{r\times n}$ 的密度是指 H 中平均每行 1 的数目，即

$$d_H = \frac{H\text{中1的数目}}{r}$$

定义 7　n -比特安全性。任何攻击者成功攻击所花费的代价（基本操作数）$T > 2^n$；或者说任何有效的攻击成功率 $\varepsilon < 2^{-n}$；再或者是以上两种情况的结合，即 $T/\varepsilon > 2^n$。

1.2　传统的 McEliece 体制

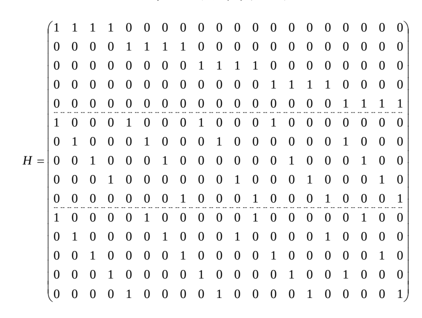
McEliece 体制[10]是在 1978 年由 McEliece 提出的基于编码理论的一种公钥密码体制。该体制加解密过程中使用到了三个矩阵，即 G，S，P，其中 G 为可以纠正 t 个错误的 $(n,k,2t+1)$ -线性码（McEliece 提出使用的线性码 Goppa 码）的 $k\times n$ 阶生成矩阵；S 为 $k\times k$ 阶随机非奇异（可逆）矩阵；P 为 $n\times n$ 阶随机置换矩阵。由此计算出矩阵 $G' = SGP$ 和纠错能力 t 一起作为公钥，私钥为 G，S，P。

加密：$c = mG' + e$，其中 e 为重量小于等于 t 的随机差错图样；

解密：等式两边同时乘 P^{-1}，即 $cP^{-1} = mSG + eP^{-1}$，然后使用 Goppa 码的快速译码算法纠出差错图样 eP^{-1}，计算出 mS，则 $m = mSS^{-1}$。

1.3　LDPC/MDPC 码的 Tanner 图表示

LDPC 码和 MDPC 码都可用 Tanner 图表示其校验矩阵，例如一个 $(20,15,4)$ -LDPC 码检验矩阵如下：



$$H=\begin{pmatrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
\hline
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
1&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1
\end{pmatrix}$$

其 Tanner 图如图 1 所示。

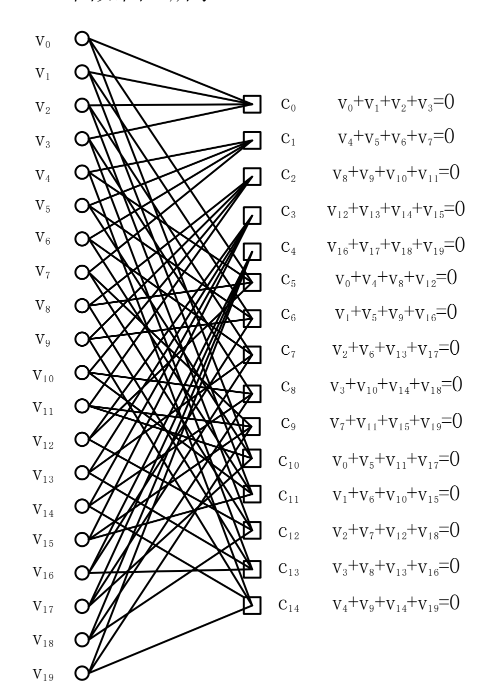


图 1　$(20,15,4)$ -LDPC 码的 Tanner 图

图 1 中 v_i 为变量节点（对应校验矩阵的行元素），其中 $i = (0,1,\cdots,19)$，c_j 为校验节点（对应校验矩阵的列），其中 $j = (0,1,\cdots,14)$，每个校验节点对应有一个校验方程，如图 1 中右侧所示。

Tanner 图大多用在迭代译码算法中。比特翻转（BF）迭代

译码的一般译码过程可以简单地概括如下：

a)接收码字 c；

b)计算校验子 $s=cH^T$；

c)对每个变量节点检查计数校验方程不满足的个数 T；

d)若有变量节点的 T 值超过了规定的阈值 b，则翻转该比特；

e)计算并检查是否所有校验方程都成立，若否，返回第二步；若是，结束译码。

2 改进方案介绍

首先对方案涉及到的主要符号进行约定，其余符号在方案介绍过程中约定。其中 n 为级联码的码长，n_1、n_2 分别为 QC-MDPC 和 QC-LDPC 的码长，k、r、w 分别为级联码的信息位长、校验位长、奇偶校验矩阵的行重，$R=(n-r)/n$ 为编码效率（码率）。

本文提出的方案包含密钥生成、加密和解密三个算法。主要改进是将 QC-LDPC 码和 QC-MDPC 码的奇偶校验矩阵结合作为私钥，生成二者的级联码字应用于 McEliece 变型方案，而且给出改进的译码算法。校验矩阵 H 由校验矩阵 H_1、H_2 组成，$H=(H_1|H_2)$，其中 H_2 可化为系统形式。则可由校验矩阵或生成矩阵决定两个码长分别为 n_1、n_2 的 QC-MDPC 码和 QC-LDPC 码，二者级联成新的码长为 $n=n_1+n_2$ 的码字。

2.1 密钥生成

a)随机生成两个分别重为 w_1 和 w_2 的向量 h_{00} 和 h_{01}，并且 $h_0=(h_{00},h_{01})\in F_2^n$ 的重量为 $w=w_1+w_2$；

b)将向量 h_0 作为校验矩阵 H 的第一行；

c)则 H 其余 $r-1$ 行可由每一块 H_{1a}、H_{2b} 的第一行各自循环移位而得，其中 $a\in(0,1,\cdots,n_{01}-1)$（$n_{01}=n_1/r$），$b\in(0,1,\cdots,n_{02}-1)$（$n_{02}=n_2/r$）。

由得到的校验矩阵 H，对其左乘 $H_{n_{02}-1}^{-1}$ 可得到其系统形式 $H=(P|I_{r\times r})$，由此可相应得 $k\times n$ 阶生成矩阵 $G=(I_{(n-r)\times(n-r)}|P^T)$，也可以表示为 $G=(G_1|G_2)$ 的形式，G_1、G_1 分别为两个码字的的可纠 t_1、t_2 个错误的生成矩阵。由于 QC-MDPC 有随机分量组成部分的存在，因此可以不用再添加加扰矩阵和置换矩阵。

2.2 加密

对消息 $m\in F_2^{n-r}$ 进行加密：

a)随机生成差错图样 $e\in F_2^n$，$w(e)\le t$ 而且前 n_1 部分至多重为 t_1，后 n_2 部分至多重为 t_2；

b)计算密文：$c=mG+e$，$c\in F_2^n$。

2.3 解密

本文提出改进的 BF 算法（new-BF）如下：

输入：$H\in F_2^{r\times n}$，$c=mG+e\in F_2^n$，最高迭代次数 $I_{\max}$。

输出：e，使得 $eH^T=0$；或译码失败。

参数：变量节点个数 i，校验节点个数 j，计数器的值 T，阈值 b，翻转个数 f。

a）初始化译码迭代次数 $I=0$，计数器 $T=0$。

b）对于 $j\in(0,1,\cdots,r)$，计算 s_j，若 s_j 全为 0，则停止迭代，输出码字；若 $s_j\ne0$，又 $i\in(0,1,\cdots,n-1)$，则第 j 个校验节点连接的 w 个变量节点对应的计数器。

c）检查计数器，若第 i 个变量节点的 $T\ge b$，则翻转第 i 位。

d）更新校验子。遍历检查第 j（$j\in(0,1,\cdots,r)$）个校验节点所连接变量节点的翻转个数 f，更新 s_j。若翻转次数 $f:f \bmod 2=1$，则更新之后的 s_j=0，则译码成功，输出翻转后的码字 $e\in\{c_i|i\in(0,1,\cdots,n-1)\}$。

e）否则，判断迭代次数 $I=I+1$，若 $I>I_{\max}$ 则终止迭代，输出译码失败；否则返回步 b）。

3 安全性能分析

3.1 困难问题

本文所提出的 McEliece 变型方案的安全性依赖于一般线性码译码问题中的陪集重量问题，此问题已被证明了是 NPC 问题[11]，可以抵抗量子攻击。

陪集重量问题：已知 F_2 域上的 $r\times n$ 矩阵 H，一个 r 维向量 s，以及正整数 t，在 F_2^n 上找到一个汉明重量 $\le t$ 的向量 e 使得 $s=He^T$。

此外，该体制是安全的，只要以下两个问题成立：a）在一个 $(n,n-r)$ 准循环线性码中纠正 t 个错误是难的；b）确定由一些块循环 $r\times n$ 阶矩阵生成的码字是否存在最小距离 $\le w$ 是难的。

这两个问题已被证明在非循环情况下是 NP-难的[12]，它们确切的状态在循环情况下是未知的。但是有一个共识：循环性本身不会使问题变得简单，这种情况和基于格的密码体制非常相像。

3.2 有关攻击

对基于编码理论的公钥密码体制的攻击，主要有结构攻击和译码攻击两种类型的攻击。结构攻击旨在密钥恢复，即直接利用公钥恢复私钥；译码攻击旨在消息恢复，即直接从密文中恢复明文。译码攻击主要是信息集译码攻击，结构攻击主要是最近提出的对 QC-MDPC 体制、QC-LDPC 体制的密钥恢复攻击[7,9]。

3.2.1 信息集译码攻击

信息集译码攻击，主要目的是通过已知公钥和截获的密文 c 找到差错向量的 k 个非 1 比特位置，使得线性码的生成矩阵 G 选择相应位置的 k 列组成的 G' 是可逆的。即，加密过程 $c=mG+e$，对 e 选取 k 位非 1 比特，G 选取相应的 k 列，使得组成的 G' 可逆，这样可以对应 c 选取 k 位，等式左右同乘 G'^{-1}，计算出明文 m。

现有较好的 MMT 算法[13]所需的工作因子为 $WF=\min_p \dfrac{C_n^w}{C_{n-k-l}^{w-p}C_{k+l-p/2}^{p/2}}$，其中 $l=\log_2 C_{k+l}^{p/2}$。这个攻击运行时间为 $O(2^{0.054n})$，即复杂度为指数函数。因此，如果码长 n 和信息位 k 选取较大，比如选择 $n=12005$，则运行时间至少为 $O(2^{648})$，

该攻击则不可行。

3.2.2 密钥恢复攻击

密钥恢复攻击，选取特殊的差错图样 e（见图 2）进行加密以及译码测试。对于 $n_0=2$，Guo 等表明只需恢复奇偶校验矩阵 H 的首行向量 h （见图 2)的前半部分向量 h_0 即可。

将此攻击直接应用在本文所提出的体制是不可行的。这是因为：

a）本文密钥 h_0 结构如图 3 所示。对于其 e 的设置，参与校验子计算的是 h_0 的一半，即 $H_{QC-MDPC}$ 首行向量与 $H_{QC-LDPC}$ 首行向量的一小部分，敌手无法得知体制中两种奇偶校验矩阵的分布及各自比例来恢复出密钥。

b）在本文所提体制中，QC-LDPC 校验矩阵的加入，因为密度相对 QC-MDPC 较小，则 $s_j=\sum_{i=1}^{n}e_ih_{ij}$ 为 0 的概率增大，不满足的校验方程的数目减少，相应译码失败概率降低。同时由文献[14]分析知，本文的译码算法依然适用，并且相对复杂度较低，最坏情况下对 QC-MDPC 的译码，可以降低译码错误概率，增大了攻击的译码复杂度。

c）另外，Guo 等人的攻击自身也有相应缺陷。一是其没有找出具体的数值表达式关系，二是在计算密钥距离谱时，其依赖的是大量的样本实验，三是区分 $d\in(0,1,\ldots,r/2)$ 是否存在于 h_0 的距离谱中的界限不明确。

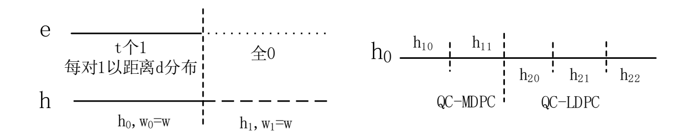


图 2　特殊的差错图样 e 以及 h　　　图 3　本文校验矩阵首行向量

对于 Fabšič 等人[9]的对 QC-LDPC McEliece 的反映攻击，一方面该攻击是利用寻找稀疏置换矩阵 Q 与软判决译码错误概率之间的相关关系为切入点进行攻击，而在本文所提出的体制中，不再对生成矩阵进行乘加扰矩阵和置换矩阵，此攻击对本文体制不可行；另一方面本文体制所用码字是由 QC-LDPC 和 QC-MDPC 级联组成，MDPC 码的引入本身增加了攻击的复杂性。

3.2.3 其他攻击

对于弱密钥攻击，Bardet 等人[15]对基于 QC-MDPC 码的公钥加密方案提出一种寻找弱密钥的方法[15]，但是此攻击不能应用在本文所提出的加密体制，因为 QC-LDPC 部分的公钥不满足其规定的弱密钥条件。对于 OTD 攻击，其是针对 QC-LDPC 体制中的 S 和 Q 展开的，因此对本文体制不可行。

4　具体参数选择和实现效率分析

4.1　参数选择

由 $c=mG+e$ 生成的码字为 $(n=n_1+n_2,r,w=w_1+w_2)$ -线性码。$r\times r$ 阶循环矩阵块 H_i 是由 r 长行向量循环移位生成，r 长行向量可以用 $F_2^n[x]/(x^r+1)$ 中的多项式表示。实际上关于 r 的选择，有一些矛盾的地方。比如，增加 r 会使得公钥变大，并且会降低计算效率；但是减少 r 又导致译码失败概率增大。对于 r 的选择，在特性上选定其为素数，因为这样可以使得 $(x^r+1)/(x+1)$ 为不可约多项式，使得可以简单地选择具有奇数权重的任何多项式来高效选择 $F_2^n[x]/(x^r+1)$ 中的可逆元素。

码长 n 和校验矩阵行重 w 的选择会影响迭代译码算法的纠错能力。迭代译码算法的纠错能力会随着码长 n 的增大而增强，随着校验矩阵行重 w 的增大而降低，因此迭代译码算法用于 QC-MDPC 体制的纠错能力低于 QC-LDPC 体制，但是适当的参数选择[6]也使 QC-MDPC 体制保证了一定的安全性。而两种码字的级联使用，由于 $w_{QC-LDPC}<w_{级联}<w_{QC-MDPC}$ 可以使纠错能力相对于 QC-MDPC 体制增强，同时因为二者码的结合又能抵抗分别对单个类型码体制的攻击而达到较高的安全性。

对于 QC-MDPC 及 QC-LDPC 体制有建议使用的参数，同时也是目前使用最普遍的参数：

a）QC-MDPC 码，文献[6]中对 MDPC 码建议的参数为码率为 $1/2$，码长和信息位大小分别为 9602 和 4801 bit，其可以提供 80 bit 安全，而且相比其他参数，此参数下公钥量最小。

b）QC-LDPC 码，Baldi 等人[5]对文献[3]进行了改进，对其参数也进行了优化，码率 $2/3$，码长和信息位大小分别为 24576 和 16384 bit。

因此，对于参数的选择（见表 1）是依据：由于需约束级联后的码长，从而使得公钥量较小，以及随机分布的存在，对 QC-MDPC 码选取建议参数的 $1/2$，同样不失安全性；对 QC-LDPC 码选取建议参数的 $1/3$，同样可以保证 80 bit 安全性。级联后的码字码率 $R=(n-r)/n=4/5$，$n=12005$，$r=2401$，$w=51$，$t=55$。同时，码率的提高，也增加了频谱利用率，使码的性能提高。

表 1　参数选择

	QC-MDPC	QC-LDPC	级联
R	$1/2$	$2/3$	$4/5$
n	4802	7203	12005
r	2401	2401	2401
w	46	5	51
t	42	13	55

4.2　密钥量及复杂度分析

4.2.1 密钥量分析

本文所提出的体制公钥为 $G\in F_2^{(n-r)\times n}$，私钥为 $H\in F_2^{r\times n}$，由于二者都是循环结构而且又都可化为系统形式，所以该体制的公钥量为 $(n_0-1)\cdot r=9604$ bit。如表 2 所示，公钥量相对于基于 Goppa 码与基于 QC-LDPC 码的 McEliece 体制大大降低，相对于基于 QC-MDPC 的 McEliece 体制稍大，但是它可以抵制对 QC-MDPC 的密钥恢复攻击。

4.2.2 复杂度分析

1）密钥生成

a）相比于 LDPC 体制和原始 McEliece 体制，本体制不再

采用矩阵 S，P 对生成矩阵加密，至少减少了 $2nk^2$ 次操作；

b)生成的奇偶校验矩阵为循环矩阵只需考虑第一行向量的选择，之后就是 r-1 次的循环移位，复杂度低；

c）对 $H^{-1}_{n_{02}-1}$ 进行计算，由于 $H_{n_{02}-1}$ 为循环矩阵，可对其使用一种矩阵求逆的高效算法[16]来求解，降低了计算操作数。

2）加密

包括码字向量与生成矩阵的乘积，以及与差错图样的相加，操作数如表 2 所示。

3)解密

使用改进的 BF 算法得到 e，纠错后再选取前 k 位得到明文。解密复杂度主要在于改进的 BF 译码算法，操作数如表 2 所示。

译码过程中对于以下几个问题的解决方法：

a）阈值 b 的计算或选择。阈值对迭代次数有很直接的影响，如果阈值太高，在每次迭代中只有很少的错误被纠正，反之，正确的比特会比错误比特翻转得多。在 Gallager 原始的比特翻转算法中，阈值 b 是在每次迭代译码之前都进行预计算，用于计算阈值的公式同时可以确保一些译码失败概率。根据 Maurich 等人[17]对几种译码方案的测试结果，此种阈值计算方法可取。因此在阈值的计算上，本文采取此种方法。

b）迭代次数的限制。经文献[17]研究发现比特翻转译码算法会在很小的迭代次数之后停止，平均大约为 3~5 次，再进行迭代对提高译码的成功率影响很小。另外文献[6]中对于迭代次数的选择建议也在 10 次以内，因为迭代次数过多会有可能导致译码失败，使译码失败概率增大。因此综合考虑，迭代次数设置为 10 以内的小整数。

c）关于校验子的更新。本文不再利用更新的码字与校验矩阵的转置相乘来重新计算校验子，而是采取检查每个校验节点所连接的变量节点的翻转次数来更新校验子的值，原方案在每一轮迭代中校验子更新这一步的计算操作数为 $n\times r$，本文改进的对校验子的更新操作数为 $w\times r$，相较减少了 $(n-w)\times r$。

表 2　与几种体制参数对比

	McEliece (original)	QC-LDPC	QC-MDPC	本文
公钥/Bytes	67072	6144	600	1200
信息位/bit	524	16384	4800	9604
码率	0.5117	0.6667	0.5	0.8
加密操作数	269336	12713984	—	7452704
解密操作数	5263360	218750976	—	28946456

5　结束语

本文基于两个不同密度奇偶校验矩阵所定义的两种码的级联码提出了一种改进的 McEliece 变型体制。分析结果表明，循环结构的加入使密钥紧致，改进的译码算法在计算复杂度上相比原译码算法有所降低，同时在安全性方面可以抵制信息集译码攻击和密钥恢复攻击。基于奇偶校验码的密码体制是后量子算法的一个很重要的方案，本文所提出的变型方案证明是可行的，今后的工作可对比特翻转译码算法的效率及安全性进行研究。

参考文献：

[1] Couvreur A, Marquez-Corbella I, Pellikaan R. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes [J]. IEEE Trans on Information Theory, 2016, PP (99): 1.

[2] Bardet M, Chaulet J, Dragoi V, *et al.* Cryptanalysis of the McEliece public key cryptosystem based on polar codes [M]. Post-Quantum Cryptography. Berlin: Springer International Publishing, 2016: 118-143.

[3] Baldi M, Chiaraluce F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes [C]// Proc of IEEE International Symposium on Information Theory. 2007: 2591-2595.

[4] Otmani A, Tillich J P, Dallot L. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes [J]. Mathematics in Computer Science, 2010, 3 (2): 129-140.

[5] Baldi M, Bodrato M, Chiaraluce F. A new analysis of the McEliece cryptosystem based on QC-LDPC codes [C]// Proc of International Conference on Security and Cryptography for Networks. Berlin: Springer-Verlag, 2008: 246-262.

[6] Misoczki R, Tillich J P, Sendrier N, *et al.* MDPC-McEliece: new McEliece variants from Moderate Density Parity-Check codes [C]// Proc of IEEE International Symposium on Information Theory Proceedings. 2013: 2069-2073.

[7] Guo Q, Johansson T, Stankovski P. A key recovery attack on MDPC with CCA security using decoding errors [M]// Advances in Cryptology. Berlin: Springer, 2016: 789-815.

[8] Shooshtari M K, Ahmadian-Attari M, Johansson T, *et al.* Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes [J]. IET Information Security, 2016, 10 (4): 194-202.

[9] Fabšič T, Hromada V, Stankovski P, *et al.* A Reaction Attack on the QC-LDPC McEliece Cryptosystem [C]// Proc of International Workshop on Post-Quantum Cryptography. Cham: Springer, 2017: 51-68.

[10] Mceliece R J. A public-key cryptosystem based on algebraic coding theory [J]. Deep Space Network Progress Report, 1978, 44: 114-116.

[11] Berlekamp E R, Mceliece R J, Van Tilborg H C A. On the inherent intractability of certain coding problems (Corresp.) [J]. IEEE Trans on Inf Theory, 1978, 24 (3): 384-386.

[12] Vardy A. The intractability of computing the minimum distance of a code [J]. IEEE Trans on Information Theory, 2002, 43 (6): 1757-1766.

[13] May A, Meurer A, Thomae E. Decoding Random Linear Codes in Õ (20. 054n) [C]// Proc of the 17th International Conference on Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 107-124.

[14] Chaulet J, Sendrier N. Worst case QC-MDPC decoder for McEliece

cryptosystem [C]// Proc of IEEE International Symposium on Information Theory. 2016: 1366-1370.

[15] Bardet M, Dragoi V, Luque J G, *et al.* Weak keys for the quasi-cyclic MDPC public key encryption scheme [M]// Progress in Cryptology. Berlin: Springer International Publishing, 2016: 346-367.

[16] Baldi M, Bambozzi F, Chiaraluce F. On a family of circulant matrices for quasi-cyclic low-density generator matrix codes [J]. IEEE Trans on Information Theory, 2011, 57 (9): 6052-6067.

[17] Maurich I V, Oder T. Implementing QC-MDPC McEliece encryption [J]. ACM Trans on Embedded Computing Systems, 2015, 14 (3): 1-27.